Amendment to the Claims:

This listing of claims will replace all versions, and listings, of claims in the application:

Listing of Claims:

1-70. (Cancelled)

71. (New) A system, comprising:

an authentication server disposed on a network;

a switch coupled to the network and communicatively coupled to the authentication server via the network; and

an access point communicatively coupled to the switch;

wherein the access point is configured to authenticate with the authentication server and establish a secure communication session with the switch;

wherein the access point is configured to send a message to the switch comprising data representative of an authenticated wireless client responsive to the authenticated wireless client successfully authenticating with the authentication server; and

wherein the access point is configured to forward all communications received from the authenticated wireless client to the switch responsive to the authenticated wireless client successfully authenticating with the authentication server.

72. (New) The system according to claim 71, the switch comprises a table of authorized users, wherein the switch updates the table of authorized users with the medium access control address of the authenticated wireless client.

73. (New) The system according to claim 71, the switch comprises a table of authorized users, wherein the switch updates the table of authorized users with the medium access control list, the quality of service parameters and the access control list of the authenticated wireless client.

74. (New) The system according to claim 71, wherein a session key is generated for subsequent communications between the authenticated wireless client and the access point responsive to the authenticated wireless client successfully authenticating with the authentication server.

75. (New) The system according to claim 71, further comprising the authentication server is responsive to establish a message authentication check key for the secure communication session between the switch and the access point.

76. (New) The system according to claim 75, wherein the a message authentication check key uniquely identifies the access point to the switch.

77. (New) The system according to claim 75, further comprising:

the access point is configured to send the data representative of the authenticated wireless client signed with the message authentication check key; and

the switch is responsive to receiving the data representative of the authenticated wireless client to verify the message authentication check key.

78. (New) The system according to claim 77, further comprising:

the switch is configured to maintain a database containing authorized media access control addresses; and

the switch is configured to verify the message with the data representative of the authenticated wireless client was sent by the access point by verifying the media access control address of the access point.

79. (New) The system according to claim 78, further comprising:

the data representative of the authenticated wireless client comprises a media access control address for the authenticated wireless client;

the switch is responsive to receiving the data representative of the authenticated wireless client to store the media access control address for the authenticated wireless client in the database; and

the switch is responsive to receiving packets from the authenticated wireless client forwarded by the access point to verify the media access control address of the packets from the authenticated wireless client with the database.

80. (New) The system according to claim 71, wherein the secure communication session is established between the switch and the access point prior to authenticating the authenticated wireless client.

81. (New) The system according to claim 71, further comprising:

the switch maintains a database of authenticated supplicants; and

the switch stores the media access control of the access point in the database responsive to the access point successfully authenticating with the authentication server.

82. (New) A system, comprising:

an authentication server disposed on a network;

a first authenticator communicatively coupled to the authentication server via the network; and

a first supplicant communicatively coupled to the first authenticator;

wherein the first supplicant is configured to authenticate with the authentication server and establish a secure communication session with the first authenticator;

wherein the first supplicant is configured to function as an authenticator for a second supplicant communicatively coupled to the first supplicant;

wherein the first supplicant is configured to send a message with data representative of the second supplicant to the first authenticator responsive to the second supplicant successfully authenticating with the authentication server; and

wherein the first supplicant is configured to forward all communications received from the second supplicant to the first authenticator responsive to the second supplicant successfully authenticating with the authentication server.

83. (New) The system according to claim 82, the first authenticator comprises a table of authorized users, wherein the first authenticator updates the table of authorized users with the medium access control address of the first supplicant.

84. (New) The system according to claim 83, further comprising the first authenticator updates the table of authorized users with an access control list and quality of service parameter for the second supplicant.

85. (New) The system according to claim 82, wherein a session key is generated for subsequent communications between the second supplicant and the first supplicant responsive to the authenticated wireless client successfully authenticating with the authentication server.

86. (New) The system according to claim 85, further comprising the authentication server is responsive to establish a message authentication check key for the secure communication session between the first authenticator and the first supplicant.

87. (New) The system according to claim 86, further comprising the first supplicant is configured to send the data representative of the second supplicant signed with the message authentication check key.

88. (New) The system according to claim 87, further comprising:

the first supplicant is configured to maintain a database containing authorized media access control addresses; and

the first supplicant is configured to verify the message with the data representative of the second supplicant was sent by the first supplicant by verifying the media access control address of the access point.

89. (New) The system according to claim 88, further comprising:

the data representative of the second supplicant comprises a media access control address for the second supplicant;

the first supplicant is responsive to receiving the data representative of the second supplicant to store the media access control address for the second supplicant in the database; and

the first authenticator is responsive to receiving packets from the second supplicant forwarded by the first supplicant to verify the media access control address of the packets from the second supplicant with the database.

90. (New) A method, comprising:

authenticating a first with an authentication server through an authenticator;

establishing a secure communication session with the authenticator responsive to a successful authentication with the authentication server;

receiving an authentication request from a second supplicant;

forwarding the authentication request from the second supplicant to the authentication server via the authenticator;

receiving a response from the authentication server via the authenticator indicating a successful authentication of the second supplicant;

sending data representative of the second supplicant to the authenticator; and

forwarding all communications received from the second supplicant to the authenticator responsive to receiving a response from the authentication server via the authenticator indicating a successful authentication of the second supplicant.

91. (New) The method according to claim 90, further comprising generating a session key for subsequent communications between the first supplicant and the second supplicant responsive to the second supplicant successfully authenticating with the authentication server.

92. (New) The method according to claim 91, further comprising establishing a message authentication check key for the secure communication session between the authenticator and the first supplicant.

93. (New) The method according to claim 92, further comprising:

the first supplicant is configured to send the data representative of the second supplicant signed with the message authentication check key.

94. (New) A method, comprising:

establishing a secure communication session with a first supplicant;

receiving data representative of a second supplicant authorized to access an associated network from the first supplicant via the secure communication session; and

allowing the second supplicant access to the associated network responsive to receiving data representative of a second supplicant authorized to access an associated network from the first supplicant.

95. (New) The method according to claim 94, further comprising:

updating a table of authorized users with the medium access control address of the second supplicant.

96. (New) The method according to claim 95, further comprising updating the table of authorized users with a quality of service parameter and the access control list for the second supplicant.

97. (New) The method according to claim 94, further comprising:

the establishing step further comprises authenticating the first supplicant with an authentication server; and

establishing a message authentication check key for the secure communication session with the first supplicant.

98. (New) The method according to claim 97, the receiving data representative of a second supplicant authorized to access an associated network further comprising verifying the data representative of the second supplicant is signed with the message authentication check key.

99. (New) The method according to claim 98, further comprising:

the table of authorized users comprises authorized media access control addresses; and

verifying the message with the data representative of the second supplicant was sent by the first supplicant by verifying the media access control address of the first supplicant with the table of authorized users.

100. (New) The method according to claim 99, further comprising:

the data representative of the authenticated wireless client comprises a media access control address for the second supplicant;

storing the media access control address for the second supplicant in the table of authorized users; and

verifying the media access control address of the packets from the second supplicant with the database responsive to receiving packets from the second supplicant forwarded by the first supplicant.